Claims

[c1]

A system for preventing analysis and monitoring of network traffic between network host computers wherein false packets are generated and transmitted along with a true packet to hide actual message traffic flow, said system comprising:

an extension header positioned in a hierarchy of Internet protocol headers controlling passage of the false packets and the true packet through a network, said extension header having a plurality of fields;

a sending host computer having means for filling said fields with values designating the size of said extension header, a message packet type, a maximum number (X) of false packets to be generated, a minimum number of hops that the false packets will traverse, a minimum and maximum and baseline false packet body size, a source address for the true packet, whether re-encryption is permitted, a false packet generation probability, a decay rate for the false packet generation probability, a total number of re-encryptions performed, and a decryption key pointer value;

means for generating at the sending host computer a plurality of false packets for each true packet; and

means for transmitting the false packets and the true packet containing said Internet protocol headers and said extension header over said network to at least one intermediate host computer and a recipient host computer.

[c2]

The system of claim 1, further including:

said least one intermediate host computer and a recipient host computer having means for generating and transmitting further false packets according to the false packet generation probability.

[c3]

The system of claim 2, further including:

means for changing the false packet generation probability using the decay rate for the false packet generation probability.

[c4]

The system of claim 3, wherein said extension header is inserted within the Internet protocol headers in the hierarchy of headers.

[c5]

The system of claim 3, wherein X is a binary number ranging from 2^0 to 2^8.

[c6]

The system of claim 4, wherein said means for generating at the sending host computer a plurality of false packets for each true packet comprises:

means for storing the value of said minimum number of hops that each false packet will traverse;

means for determining if the number of false packets (X) is > 0;

means for decrementing X;

means for determining the size of each false packet body using the baseline false packet body size as a reference;

means for determining if each false packet body size satisfies the minimum and maximum size limits designated in said fields;

means for setting the value of all said fields to 0, means for copying the values of selected fields from the true packet into the extension header for a false packet, and means for filling said baseline false packet body size with random values;

means for selecting a recipient host address for each false packet;

means for determining if the selected recipient host address satisfies the minimum number of hops for each false packet;

means for designating the message packet type; and

means for encrypting said fields for each false packet.

[c7]

The system of claim 6, further including:

means for generating a random number of false packets to be transmitted from the sending host computer;

means for generating a random number of false packets to be transmitted from the recipient host computer;

means for generating a random minimum number of hops that each false packet will traverse;

means for generating a random minimum number representative of the body size of each said false packet;

means for randomly determining whether over-encryption of each said false packet body is permitted; and

means for generating a random number representative of the false packet generation probability and decay rate for the false packet generation probability for each said false packet.

[c8]

The system of claim 2, wherein said at said at least one intermediate host computer and said recipient host computer having means for generating and transmitting further false packets according to the false packet generation probability comprises:

means for storing values of all said fields;

means for determining from said values whether re-encryption of the message packet is permitted;

means for generating a random number and comparing it to the value in said fields indicative of the re-encryption probability, means for re-encrypting the false packet body, means for incrementing the total number of re-encryptions performed, means for

appending the decryption pointer to the value in said fields, and means for increasing the value in said fields of the size of the extension header, and determining if (X) > 0;

means for decrementing X;

means for determining a size of a new false packet body using said values as a guide;

means for determining from said values whether the size of the new false packet body satisfies minimum and maximum size limits in said fields;

means for designating the message packet type; and

means for encrypting said fields for each new false packet.

[c9]

The system of claim 8, further including:

means for repeatedly decrementing X, determining a size of a new false packet body using said values as a guide, determining from said values whether the size of the new false packet body satisfies minimum and maximum size limits in said fields, selecting the message packet type, and encrypting said fields for each new false packet, until X = 0.

[c10]

A method for preventing network data packet switching traffic analysis by generating and transmitting false packets along with a true packet to hide actual message traffic flow, comprising the steps of:

a. inserting an extension header having a plurality of fields in a hierarchy of Internet protocol headers controlling passage of the false packets and the true packet through a network;

b. at a sending host computer, filling said fields with values designating the size of said extension header (0), a message packet type (A), a maximum number (X) of false packets to be generated (B), a minimum number of hops that the false packets will traverse (C), a minimum (D) and maximum (E) and baseline (F) false packet body size, a

source address (G) for the true packet, whether re-encryption is permitted (H), a false packet generation probability (I), a decay rate for the false packet generation probability (J), a total number of re-encryptions performed (M), and a decryption key pointer value (N);

c. generating at the sending host computer a plurality of false packets for each true packet;

d. transmitting the false packets and the true packet containing said Internet protocol headers and said extension header over said network;

e. at an intermediate and recipient host computer, decrypting the extension header and determining whether the packet is true or false;

f. if false, determining from the false packet generation probability whether to generate a new false packet;

g. changing the false packet generation probability using the decay rate for the false packet generation probability;

h. decrementing X and filling said fields with values designating the new false packet;

i. transmitting the new false packet containing the extension header to a subsequent host computer; and

j. repeating steps h. and i. until X = 0.

[c11]

A method according to claim 10, wherein said step of generating at the sending host computer a plurality of false packets for each true packet further includes:

a. storing the value of said minimum number of hops that each false packet will traverse;

b. determining if the number of false packets (X) is > 0;

c. if yes, decrementing X;

d. determining a size of the false packet body using the baseline false packet body size (F) as a reference;

e. determining if the false packet body size satisfies the minimum (D) and maximum (E) size limits designated in said fields;

f. if yes, setting the value of all said fields to 0, copying the values for selected fields from the true packet into the extension header for a new false packet, and filling said new false packet body with random values;

g. selecting a recipient host address for the new false packet;

h. determining if the selected recipient host address satisfies the required minimum number of hops (C);

i. if yes, selecting the message packet type (A);

j. filling said fields with values designating the new false packet;

k. transmitting the new false packet; and

l. repeating steps c through k until X = 0.

[c12]

A method according to claim 10, wherein said step of filling said fields further includes:

a. generating a random number for the false packets to be transmitted from the sending host computer;

b. generating a random number for the false packets to be transmitted from the recipient host computer;

c. generating a random number for the hops that each false packet will traverse;

d. generating a random number representative of the body size of each said false packet;

e. randomly determining whether over-encryption of each said false packet body is permitted; and

f. generating a random number representative of the false packet generation probability and the decay rate for the false packet generation probability for each said false packet.

[c13]

The method of claim 10, further including the step of inserting the extension header within the Internet protocol headers in the hierarchy of headers.

[c14]

The method of claim 10, wherein said step of transmitting from the intermediate and recipient host computer a new false packet further includes:

a. storing values of all said fields;

b. determining from said values whether re-encryption of message packets is permitted;

c. if yes, generating a random number and comparing it to the value in said fields indicative of the re-encryption probability;

d. if said random number is greater than the re-encryption probability, re-encrypting the false packet body, incrementing the total number of re-encryptions performed (M), appending the decryption key pointer to the value in (N), increasing the value of the size of the extension header (0), and determining if (X) > 0;

e. if yes, decrementing X

f. determining a size of the new false packet body using the baseline false packet body size (F) as a reference;

g. determining from said values whether the size of the false packet body satisfies the minimum (D) and maximum (E) size limits in said fields;

h. filling said extension header with the stored values of all said fields and transmitting said new false packet containing said extension header to another host computer; and

i. repeating the steps e. through h. until X = 0.

[c15]

A method for preventing network data packet switching traffic analysis by generating and transmitting false packets along with a true packet to hide actual message traffic flow, comprising the steps of:

a. inserting an extension header having a plurality of fields in a hierarchy of Internet protocol headers controlling passage of the false packets and the true packet through a network;

b. at a sending host computer, filling said fields with values designating the size of said extension header (0), a message packet as true or false (A), a maximum number (X) of false packets to be generated (B), a minimum number of hops that the false packets will traverse (C), a minimum (D) and maximum (E) and baseline (F) false packet body size, an address (G) for the true packet, whether re-encryption is permitted (H), a false packet generation probability (I) a decay rate for the false packet generation probability (J), a total number of re-encryptions performed (M), and a decryption key pointer value (N);

c. generating at the sending host computer a plurality of false packets for each true packet; and

d. transmitting the false packets and the true packet containing said Internet protocol headers and said extension header over said network to at least one intermediate and a recipient host computer.

[c16]

The method of claim 15, further including the steps:

a. at the intermediate and recipient host computers, decrypting the extension header and determining whether the packet is true or false;

b. if false, determining from the false packet generation probability whether to generate a new false packet;

c. if true, setting X to the value in (B);

d. decrementing X and filling said fields with values designating the new false packet;

e. transmitting the new false packet containing the extension header to a subsequent host computer; and

f. repeating steps b. through e. until X = 0.

[c17]

A method according to claim 15, wherein said step of generating at the sending host computer a plurality of false packets for each true packet further includes:

a. storing the value of said minimum number of hops that each false packet will traverse;

b. determining if the number of false packets (X) to be sent is > 0;

c. if yes, decrementing X for each false packet transmitted;

d. determining the size of the false packet body using the baseline false packet body size (F) as a reference;

e. determining if the false packet body size satisfies the minimum (D) and maximum (E) size limits designated in said fields;

f. if yes, setting the value of all said fields to 0, copying the values for selected fields from the true packet into the extension header for the new false packet, and filling said new false packet body with random values;

g. selecting a recipient host address for the new false packet;

h. determining if the selected recipient host address satisfies the minimum number of hops (C);

i. if yes, designating the message packet type (A);

j. filling all remaining fields with values designating the new false packet; and

k. transmitting the new false packet.

[c18]

A method according to claim 15, wherein said step of filling said fields further includes:

a. generating a random number of false packets to be transmitted from the sending host computer;

b. generating a random number of false packets to be transmitted from the recipient host computer;

c. generating a random number for the minimum number of hops that each false packet will traverse;

d. generating a number representative of the minimum and maximum body size of each said false packet;

e. randomly determining whether over-encryption of each true or false packet body is permitted; and

f. generating a random number representative of the false packet generation probability and decay rate for the false packet generation probability for each said false packet.

[c19]

The method of claim 15, further including the step of inserting the extension header within the Internet protocol headers in the hierarchy of headers.

[c20]

The method of claim 16, wherein said step of transmitting from the intermediate and recipient host computer a new false packet further includes:

a. storing values of all said fields;

b. determining from said values whether re-encryption of message packets is permitted;

c. if yes, generating a random number and comparing it to the value in said fields indicative of the re-encryption probability;

d. if said random number is greater than the re-encryption probability, re-encrypting the false packet body, incrementing the total number of re-encryptions performed (M), appending the decryption key pointer to the value in (N), increasing the value of the size of the extension header (0); and determining if (X) > 0;

e. if yes, decrementing X

f. determining a size of the new false packet body using the baseline false packet body size (F) as a reference;

g. determining from said values whether the size of the false packet body satisfies the minimum (D) and maximum (E) size limits in said fields;

h. filling said extension header with the stored values of all said fields and transmitting said new false packet containing said extension header to another host computer; and

i. repeating the steps e. through h. until X = 0.